Preparer Note (PN):

This document contains instructions in blue hidden text. To view hidden text, click on the ¶ (Show/Hide) icon on your tool bar. If that doesn't work, see the document "How to View Hidden Text" on the Exhibit G website at http://int.lanl.gov/security/ExG.shtml. There is no need to delete the blue hidden text instructions since hidden text will not affect the formatting of the printed document and will not print unless the application's default setting is changed.

Asterisks highlighted in yellow (i.e., *) have been used throughout this document as placeholders to indicate where information is to be inserted.

Make sure that you update the table of contents before releasing this document. To update the table of contents, place your cursor anywhere within the Table of Contents section shown below and click your left mouse button, press the "F9" button on your keyboard, select "Update entire table", and click "OK". Your table of contents will automatically be updated.

Make sure to delete this note in its entirety, before releasing this document.

EXHIBIT G
SECURITY REQUIREMENTS
TABLE OF CONTENTS

G1.0 Definitions and Acronyms (May 2014)

Definitions and acronyms may be accessed electronically at
http://www.lanl.gov/resources/_assets/docs/Exhibit-G/exhibit-g-definitions-acronyms-green.pdf

G2.0 Security Requirements (May 2014)

SUBCONTRACTOR shall comply with all requirements specified in this exhibit. All measures taken by CONTRACTOR to correct Subcontract Workers' non-compliance shall be at SUBCONTRACTOR'S expense, and the cost thereof, including any stipulated penalties resulting from such non-compliance, shall be deducted from payments otherwise due SUBCONTRACTOR. Additionally, when requested by CONTRACTOR, SUBCONTRACTOR shall provide such information, assistance and support as necessary to facilitate CONTRACTOR'S compliance with any DOE Directives that may be applicable to the scope of work.

2.1 DEAR Clauses Incorporated By Reference

2.1.1 The Department of Energy Acquisition Regulation (DEAR) clauses which are incorporated by reference herein shall have the same force and effect as if printed in full text.

2.1.2 Full text of the referenced clauses may be accessed electronically at http://farsite.hill.af.mil/VFDOE1.htm

2.1.3 The following alterations apply only to FAR and DEAR clauses and do not apply to DOE or NNSA Directives. Wherever necessary to make the context of the unmodified DEAR clauses applicable to this subcontract:

- The term "Contractor" shall mean "SUBCONTRACTOR;"
- The term "Contract" shall mean this subcontract; and
- The term "DOE", "Government," "Contracting Officer" and equivalent phrases shall mean CONTRACTOR and/or CONTRACTOR'S representative, except the terms "Government" and "Contracting Officer" do not change when a right, act, authorization or obligation can be granted or performed only by the Government or the prime contract Contracting Officer or his duly authorized representative; or where specifically modified herein.

2.1.4 The following clauses apply as stated in the Instructions.

Clause Number	Title and Date	Instructions
DEAR 952.204-2	Security (May 2002)	Applies when work involves or may involve classified information, access to special nuclear materials or the provision of protective services.
DEAR 952.204-70	Classification / Declassification (Sep 1997)	Applies when work involves or may involve access to classified information.
DEAR 952.204-73	Facility Clearance (May 2002)	Applies when Subcontractor employees/workers are required to possess access authorizations.
CFR 952.247-70	Foreign Travel (Dec 2000)	Applies if foreign travel may be required in order to perform subcontract work. If applicable, authorization is required from DOE prior to traveling.
DEAR 952.204-77	Computer Security (Aug 2006)	Applies when Subcontractor has access to computers owned, leased or operated on behalf of the DOE.
DEAR 970.5204-1	Counterintelligence (Dec 2000)	Applies when DEAR 952.204-2 Security and DEAR 952.204-70 Classification / Declassification are applicable.
FAR 52.204-9	Personal Identity Verification of Contractor Personnel (Jan 2011)	Applies when Subcontractor has routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system.

2.2 DOE Directives Incorporated by Reference

When requested by CONTRACTOR, SUBCONTRACTOR shall provide such information, assistance and support as necessary to ensure CONTRACTOR'S compliance with the following DOE/NNSA Directives, as applicable to the scope of work. SUBCONTRACTOR shall comply with the requirements of the Contractor Requirement Document (CRD) attached to a Directive when required by such CRD. The Directives are prefaced with certain conditions for applicability to the subcontract. A referenced Directive does not become effective or operative under this subcontract unless and until the conditions precedent are met through the scope of work. The DOE Directives referenced herein may be found at http://www.directives.doe.gov/ Applicable NNSA NAP documents may be provided to SUBCONTRACTOR by the Contract Administrator / Procurement Specialist (CA/PS) upon request.

Clause Number	Title	Instructions
DOE O 142.2A	Voluntary Offer Safeguards Agreement and Additional Protocol with the International Atomic Energy Agency	Applies to contracts which involve activities potentially subject to application of safeguards by the International Atomic Energy Agency (IAEA)
DOE M 142.2-1	Manual for Implementation of the Voluntary Offer Safeguards Agreement and Additional Protocol with the IAEA.	Applies if contract involves activities associated with the IAEA Safeguards Agreement.
DOE O 142.3A	Unclassified Foreign Visits and Assignment	Applies if contract involves foreign national access to DOE-owned or leased sites/facilities. Applies if contract involves off-site foreign national access to DOE information or technologies that are not releasable to the public.
NAP 14.1C, Chpt. VII	NNSA Baseline Cyber Security Program, Chapter VII Incident Management	Applies if contract work involves information systems used on behalf of DOE/NNSA to collect, process, store, display, create, disseminate or transmit national security or unclassified DOE / government information.
NAP 14.1D	Baseline Cyber Security	Applies if contract involves National Security Systems that collect, process, store, display, create, disseminate, or transmit information.
DOE O 205.1B Chg 1	Department of Energy Cyber Security Program	Applies if contract includes access to DOE unclassified or classified information and information systems used or operated by CONTRACTOR.
DOE O 452.4A	Security and Control of Nuclear Explosives and Nuclear Weapons	Applies if contract includes work in support of the Nuclear Explosive and Weapon Security and Control Program.
DOE O 452.8	Control of Nuclear Weapon Data	Applies if contract work requires workers to hold a clearance and have a need to know to perform in authorized government function.
DOE O 457.1	Nuclear Counterterrorism	Applies if contract involves or could potentially involve accessing or generating nuclear weapon design information.
DOE M 457.1-1	Control of Improvised Nuclear Device Information	Applies if contract involves or could potentially involve accessing or generating improvised nuclear device information.
DOE O 460.2A	Departmental Materials Transportation & Packaging Management	Applies if contract involves transportation and packaging of hazardous or nonhazardous material.
DOE M 460.2-1A	Radioactive Material Transportation Practices Manual	Applies if contract involves transportation and packaging of radioactive material or radioactive waste.
DOE O 461.2	Packaging and Transfer of Materials of National Security Interest	Applies if contract includes packaging and shipment off-site of materials of national security interest.

Clause Number	Title	Instructions
DOE M 470.4B Chg 1	Safeguards and Security Program	Applies when contract requires security training and/or requires a FOCI determination for access authorizations (clearances).
DOE O 473.3	Protection Program Operations	Applies if contract includes responsibilities for operating, administering, and/or protecting DOE & NNSA safeguards and security interests.
DOE O 471.6 Chg 1	Information Security	Applies if contract includes access to unclassified or classified information and matter controlled by statues, regulation or NNSA policies.
DOE M 474.2 Chg 2	Nuclear Material Control and Accountability	Applies if contract includes access to nuclear or special nuclear material or data.
DOE O 471.1B	Identification and Protection of Unclassified Controlled Nuclear Information	Applies to work activities that may generate, possess, or have access to information or matter containing UCNI.
DOE O 471.3	Identifying Official Use Only Information	Applies if contract involves activities where Official Use Only (OUO) information and documents will be handled, used or generated.
DOE M 471.3-1	Manual for Identifying and Protecting Official Use Only Information	Applies if contract involves activities where Official Use Only (OUO) information and documents will be handled, used or generated.
DOE O 472.2 Chg 1	Personnel Security	Applies if contract work requires employees to hold a clearance and/or when official duties require access to classified information or matter, or special nuclear material or data.
DOE O 475.1	Counterintelligence Program	Applies if contract work involves access to or use of DOE facilities, technology, personnel, unclassified sensitive information and classified matter.
DOE O 475.2A	Identifying Classified Information	Applies if contract work includes access to classified information, documents, or material.
DOE O 551.1D	Official Foreign Travel	Applies if contract work involves or could potentially involve official foreign travel.
DOE O 5639.8A	Security of Foreign Intelligence Information and Sensitive Compartmented Information Facilities	Applies if contract work requires access, receipt, storage, processing and/or handling of Foreign Intelligence Information.
NAP 14.3-B	Transmission of Restricted Data Over Secret Internet Protocol Router Network (SIPRNet)	Applies if contract involves the collection, creation, processing, transmission, storage or dissemination of classified DOE or NNSA information on SIPRNet.
NAP 23	Atomic Energy Act Control of Import and Export Activities	Applies if contract involves or could potentially involve CONTRACTOR Tier 2 specifications that reveal a specific nuclear weapon function or nuclear weapon tests and explosions.

2.3 Goal of Zero Security Incidents

SUBCONTRACTOR and any lower-tier subcontractors shall strive to eliminate all security events, incidents, and adverse impacts to national security.

2.4 Cloud Computing Services If SUBCONTRACTOR anticipates using cloud computing services in the performance of this subcontract, additional security requirements for using those services shall apply as outlined under Section G7.0 Cyber Information Security.

G3.0 General Security (May 2014)

3.1 Work site, Security Area, Badge and Data Information

WORK SITE / TA:	
	DOE owned/leased (LANL) or LANS' owned/leased facility or property
	Subcontractor owned/leased and DOE Owned / Leased (LANL) facility or property
	Subcontractor owned/leased only

TYPE / CATEGORY	
	Subcontract
	Subcontract Master Task Order
	Subcontract Task Order / Release
	Purchase Order (will not become a Subcontract)

ON-SITE WORK AREA DESIGNATION	
	General Access Area / Publically Accessible
	Property Protection Area (PPA)
	Limited Area (LA)
	Protection Area (PA)
	Material Access Area (MAA)
	SCIF, SAPF, certified Vault or Vault Type Room

BADGE TYPE / CLEARANCE LEVEL	
	LANL Generic Uncleared US Visitor badge
	LANL Generic Uncleared US Visitor Escort Required badge
	LANL Uncleared Site-specific badge
	LANL Uncleared Foreign National badge
	LANL Cleared Foreign National badge
	Uncleared DOE badge
	L-Cleared DOE badge
	Q-Cleared DOE badge
	HRP

DATA CLASSIFICATION	
	Classified
	UCNI
	Controlled Unclassified (OUO, LPI, PII, ECI, AT, NNPI, RSI)
	Unclassified
	Unclassified / Public Release

OPSEC PLAN	
	Required
	Not Required

CYBER SECURITY PLAN	
	Required
	Not Required

3.2 Integrated Safeguards and Security Management (ISSM)

ISSM uses a five-step process as the system to perform work securely. ISSM provides a framework to support each worker in fulfilling their security responsibilities. The following five-step process defines a systematic approach to actions taken before, during, and after work is performed. SUBCONTRACTOR shall ensure that the ISSM five-step process (or an equivalent process) is followed by all Subcontract Workers.

(1) Define the Scope of Work.

(2) Analyze the Security Risk.

(3) Develop and Implement Security Controls.

(4) Perform Work within Security Controls.

(5) Ensure Performance.

3.3 Safeguards, Security and Counterintelligence Awareness

3.3.1 Operations Security (OPSEC) Plan

SUBCONTRACTOR shall develop, with assistance from CONTRACTOR'S Operations Security Program Office, implement and sustain a DOE OPSEC Plan using the template provided by the Contract Administrator / Procurement Specialist. SUBCONTRACTOR'S OPSEC Plan shall be approved by CONTRACTOR'S Office of Counterintelligence, Operations Security Program Office before work may begin at LANL. A link to the OPSEC Plan template is http://www.lanl.gov/resources/exhibit-g.php

3.3.2 SUBCONTRACT workers shall report all of the following situations to the Office of Counterintelligence and inform the RLM or STR/AdSTR and CA / PS.

- Professional contacts and relationships with sensitive country foreign nationals, whether they occur at one's worksite or abroad.
- All unofficial travel to any DOE sensitive country at least 30 days before departure. *(Form 1743)*
- All official travel to any DOE sensitive country at least 30 days before departure. Coordinate with LANL host to fill out the necessary paperwork.
- Any suspicious or provocative actions encountered while on travel.
- Suspicious or provocative actions or behaviors on the part of foreign nationals visiting or assigned to LANL.
- Substantive personal relationships with sensitive country foreign nationals (who are not lawful permanent residents), other than family members.
- Business transactions including financial transactions, partnerships, or other business interests or investments with citizens of sensitive countries who are not lawful permanent residents, whether they involve one-time interactions or ongoing financial relationships. (Small payments for things such as house cleaning or other such personal services or financial support provided to family members are not included).
- Any attempts by unauthorized persons to gain access to classified information. (Not limited to DOE sensitive country foreign nationals or foreign nationals; includes US and non-US citizens)

3.3.3 SUBCONTRACTOR shall be alert to and report any of the following to the RLM and STR/AdSTR:

- attempts by unauthorized persons to obtain information;
- unexplained / excessive use of copiers by workers;
- workers living beyond their means;
- unusual foreign travel patterns of workers; and
- personal problems of workers that could affect security or fitness for duty.

3.4 Security Training

3.4.1 SUBCONTRACTOR shall ensure that all Subcontract Workers:

- become familiar with the Integrated Safeguards and Security Management (ISSM) process and its implementation requirements for the work to be performed and their

security responsibilities; and

- complete required safeguards, security and cyber-security training as indicated herein.

3.4.2 The training matrix below identifies security training Subcontract Workers may be required to complete before beginning work at LANL. An "X" before the name of the course indicates that such training is required under this subcontract.

SUBCONTRACTOR management shall review the security requirements indicated below with each worker. A signed official copy of the review and acceptance by the subcontract worker shall be kept on file with SUBCONTRACTOR. Each subcontract worker's security requirements shall be reviewed with management yearly or whenever the worker's job security duties change.

Required Course	Course Title - Required For	Frequency	Estimated Time to Complete Training
General Security			
	General Employee Training (GET) - New Hires / Live or web	Once	8 hrs.
	LANL Emergency Procedures and Protective Actions – All / web	12 months	10 min.
	Graded-Approach GET Training - Green Field Construction / video	Once	1 hr.
	Facility Security Officer Orientation – for a FOCI Determination / web	Once	2 hrs.
	Annual Security Refresher (ASR) – L & Q-cleared Workers / web	12 months	1 hr.
	Comprehensive Security Briefing - L & Q-cleared Workers / web	Once	2 hrs.
	Export Control Fundamentals – Based on SOW / web	12 months	30 min.
	Substance Abuse Awareness – All / web	Once	30 min.
	Last Angry Words (Workplace Violence) – All / web	Once	15 min.
Classified Matter Protection And Control			
	Classified Parts Procedures Self-Study - Classified Parts Custodians/ web	Once	30 min.
	CMPC for Custodians - Classified Matter Custodians (CMCs) & Classified Library Custodians (CLCs) / live	Once	2 days - 16 hrs.
	Classified Matter Protection - Classified Matter Users / web	Once	2 hrs.
	CMPC User Refresher - Classified Matter Users / web	24 months	1 hr.
	Sigma Awareness Self-study - Classified Doc Custodians / web	12 months	1 hr.
	CMPC for Custodians Quiz - CMCs & CLCs / live	Once	2 days
	CMPC CMC Refresher Training - CMCs & CLCs / web	24 months	1 hr.
Cyber Information Security			
	Initial Information Security Briefing - All Computer Users / web	Once	1 hr.
	Annual Information Security Refresher – all Computer users / web	12 months	30 min.
	Classified Computer Security - Classified Computer Users / live	Once	4 hrs.
	ISSO Training - Computer System Security Officers (ISSOs) / live	Once	2.5 hrs.
	ISSO Refresher Training - ISSOs / live	12 months	2 hrs.
	IMP 313 Roles, Responsibilities, Authority and Accountability - ISSOs & Organizational Computer Security Representatives (OCSRs) / web	Once	1 hr.
	P219 Cyber Security Risk Management - ISSOs and OCSRs / web	Once	45 min.
	OCSR Fundamentals – OCSRs / live	Once	2.5 hrs.
	OCSR Refresher Training - OCSRs / live	12 months	2.0 hrs.
Human Reliability Program			
	HRP for Managers - Supervisors / web	12 months	30 min.
	HRP Training for HRP Workers - workers / web	12 months	20 min.
Protecting Classified & Sensitive Information			
	DC Orientation Phase 1 - Derivative Classifiers (DCs) / web	Once	1 hr.
	DC Phase II - DCs / live	Once	4 hrs.
	Authorized DC Recertification - DCs / live	36 months	2 hr.

Required Course	Course Title - Required For	Frequency	Estimated Time to Complete Training
	Protecting UCNI - Users of Unclassified Controlled Nuclear Information (UCNI) / web	Once	1 hr.
	Sigma 14 Awareness - Sigma-authorized Workers / web	12 months	1 hr.
	Sigma 15 Awareness - Sigma-authorized Workers / web	12 months	1 hr.
	Sigma 20 Awareness - Sigma-authorized Workers / web	12 months	1 hr.
Nuclear Material Control And Accountability			
	LANMAS & LAMCAS User - workers doing LANMAS data entry / live	Once	8 hrs.
	MBA Custodian - MBA Custodians / live	Once	2 hrs.
	NM Custodian Refresher - MBA Custodians / web	12 months	2 hrs.
	NM Handler Awareness - NM Handlers / web	24 months	4 hrs.
	NM Physical Inventory - MBA Custodians / web	12 months	1.5 hrs.
	Tamper Indicating Devices (TID) – TID Custodian / Users / live	Once	8 hrs.
	TID Requalification - TID Custodian/Users / web	24 months	3 hrs.
Physical Security			
	Escort Responsibilities - Escorts & Vault or Vault Type Room Users, Custodians / web	12 months	30 min.
	Key Custodian - Key Core Custodians / Alternates / web	12 months	1 hr.
	The Outsider - Vault or Vault Type Room Users (AIS Escorts) / web	Once	1 hr.
	Vault or Vault Type Room Custodian - Vault or Vault Type Room Custodians / web	12 months	10 min.
	Vault or Vault Type Room User - Vault or Vault Type Room Users / web	12 months	10 min.
	Vault or Vault Type Room RLM – Managers / web	12 months	10 min.
Self-Assessments			
	S&S Self-Assessment Training - Security Subject Matter Experts / web	Once	1 hr.
Site-Specific Training			

3.5 Security Stop Work

When any Subcontract Worker observes a security related hazard or unmitigated risk, the worker has the authority and responsibility to inform any worker engaged in that work that the work be stopped.

3.6 Reporting Security Incidents

This subsection contains requirements for identifying and reporting known and potential incidents of security concern. Such incidents may involve issues associated with Personally Identifiable Information (PII), classified matter, computer systems, nuclear materials, secure communications, personnel security, and physical security occurring on LANL property, Laboratory-leased property or SUBCONTRACTOR-owned property. Subcontract workers shall comply with the following requirements.

3.6.1 Immediately upon discovery of a potential incident of security concern, report such concern to the Security Incident Team (SIT) (505-665-3505) or a SPL / DSO; and inform the RLM, and STR/AdSTR. During normal business hours, notifications shall be made only in person or through secure communications (STU or STE) as required below. A non-secure telephone, non-secure fax, non-secure voice mail, or non-secure electronic mail shall not be used to report a potential incident of security concern.

3.6.1.1 The potential compromise of PII shall be reported *immediately* upon discovery to the SIT or SPL / DSO. A potential compromise of PII is considered a serious information security incident because of the possibility of significant adverse consequences to the individual whose data has been compromised.

3.6.1.2 *Immediately* report all security incidents and potential threats and vulnerabilities

involving LANL data utilized by the SUBCONTRACTOR to the SIT or SPL / DSO, and then notify the appropriate ISSO or OCSR, RLM and STR/AdSTR.

3.6.1.3 After discovery of any incident involving the loss, compromise, or unauthorized disclosure of classified matter, report the incident *immediately* to the SIT or SPL / DSO, then inform the assigned OCSR, RLM and STR/AdSTR.

3.6.1.4 After discovery of any incident involving the loss, theft, diversion, or unauthorized use of nuclear material, report the incident *immediately* to Material Control & Accountability Group or the SIT or SPL / DSO.

3.6.2 Contact Requirements Outside of Normal Business Hours

For all incidents contact the ADSS duty officer through the Protective Force at 505-665-7708, *immediately* after discovery of a potential incident of security concern. The ADSS on-call duty officer (505-949-0156) may ask to meet with the SUBCONTRACTOR in person so that SUBCONTRACTOR may report such known or potential incidents of security concern, if secure communications are not available.

3.7 Workplace Violence

LANL maintains a work environment that is free from violent behavior and threats of violence. Violent behavior and threats of violence are unacceptable conduct and are prohibited. Any subcontract worker who participates in workplace violence will be barred from the LANL worksite and their employer shall be notified. Workplace violence is behavior that involves:

- hostile or aggressive physical contact with another person;
- a statement or body gesture that threatens harm to another person; or
- a course of conduct that would cause a reasonable person to believe that they are under threat of harm.

G4.0 Physical Security (Feb 2014)

4.1 Prohibited Articles

Prohibited Articles are those items never permitted on DOE property (e.g. LANL), which includes leased facilities and parking lots. SUBCONTRACTOR shall ensure that prohibited articles are not brought on to DOE property. Introducing an unauthorized prohibited article onto DOE property is a reportable security incident that may result in legal action. Prohibited articles include:

- Dangerous weapons (e.g., guns and knives), explosives, or other instruments or material likely to cause substantial injury or damage to persons or property; includes pocket, hunting or other sharp knives with blades longer than 2.5 inches;
- Non-government-owned firearms;
- Alcoholic beverages, including unopened bottles or cans;
- Controlled substances such as illegal drugs and associated paraphernalia, including medical marijuana but not other prescription medicine; and
- Items prohibited by local, state or federal law.

4.2 Escorting

In addition to any facility-specific escorting requirements, SUBCONTRACTOR shall ensure that all LANL escorting requirements listed below are complied with while in a Security Area (including Property Protection Areas) whether escorting individuals or being escorted by another individual.

An Activity Security Plan (ASP) shall be developed by the LANL host when escorting in PPAs will be outside normal operating hours. SUBCONTRACTOR shall comply with all ASP requirements.

4.2.1 Uncleared foreign nationals are allowed unescorted in publicly-accessible Laboratory property only.

Uncleared foreign nationals are not permitted in Security Areas and only under extraordinary circumstances should an exception be requested. Uncleared foreign nationals may only be escorted into a security area if prior approval has been obtained from DOE/HQ and local security officials. This process takes a minimum of eight (8) weeks.

4.2.2 An Uncleared US citizen may be authorized for escorted access into a Security Area only if such individual:

- is entering an area to conduct official LANL business that can be accomplished only in a Security Area, or
- has a skill or ability that is required and cannot be provided by another person who has the required clearance (i.e., access authorization) level.

4.2.3 The following individuals shall be escorted in a Security Area:

- Uncleared US citizens;
- US citizen visitors who do not have a cleared DOE-standard badge; and
- L-cleared US citizens in a Q-Only Security Area.

4.2.4 All US citizens escorted into a Security Area shall wear one of the following:

- An Uncleared DOE standard badge;
- A LANL Generic Uncleared US Citizen Visitor Badge or;
- A LANL Generic Uncleared US Citizen ESCORT REQUIRED Visitor Badge.

4.2.5 Subcontract workers who are being escorted shall:

- Provide a valid photo ID;
- State their country of citizenship for their escort before entering a security area;
- Log in, pursuant to the manner required by the LANL owning / tenant organization, before entering a security area or a PPA controlled by an electronic badge reader;
- Physically remain with his or her escort upon entry, during the visit and upon exit of a security area.
- Comply with all requirements outlined by the escort;
- Display a valid badge at all times.

4.2.6 Subcontract Workers serving as escorts have the following responsibilities:

- Complete “Escort Responsibilities” training course prior to escorting individuals;
- Be a US Citizen and possess a valid DOE badge and clearance level for the Security Area being accessed;
- Ensure the Visitor being escorted has a valid photo ID prior to issuing any badge;
- Ensure each individual being escorted is a US citizen through their statement of such status;
- Provide Visitor with clear instructions on the rules of behavior and consequences for failure to comply, before granting access to facilities and/or information systems;
- Confirm that each Visitor displays their assigned badge whenever in a Security Area;
- Review prohibited and controlled article restrictions with each Visitor prior to escorting such visitor;
- Protect classified and unclassified controlled matter, information or discussions from unauthorized access by a Visitor;
- Log in each Visitor by whatever method is provided at the facility being accessed;
- Notify area occupants of the presence of an Uncleared Visitor;
- Maintain control of each Visitor at all times;
- Implement any facility-specific escorting requirements as required;
- Immediately notify the Requester/RLM and STR/AdSTR of any incident of security concern;
- Escort each Visitor safely to the organization’s designated muster area in the case of an emergency evacuation.

4.2.7 An escort shall not escort more than five (5) individuals at any one time, unless otherwise approved by CONTRACTOR in writing.

4.2.8 In cases where an individual without proper security clearance is discovered unescorted in

a Security Area, SUBCONTRACTOR shall immediately place such individual under escort by an authorized escort and report the situation to the RLM and STR/AdSTR as soon as possible.

4.3 Security Areas

SUBCONTRACTOR shall comply with all requirements for designated Security Areas. In addition, SUBCONTRACTOR shall ensure that all Subcontract Workers:

- Have the appropriate clearance (i.e., access authorization) for the Security Area or be properly escorted within the Security Area;
- Adhere to the posted requirements for entering any Security Area (clearance status, badge, access status, training, inspections, controlled articles, prohibited articles, etc.);
- Immediately report physical security and access control discrepancies to the SIT and RLM. Inform the STR/AdSTR. (e.g. breaches of fences or walls or attempts to circumvent security barriers);
- Use a valid badge to enter a Security Area and display the valid badge at all times photo side out, above the waist and in front of the body while in that area;
- Not introduce prohibited articles into Security Areas;
- Obtain authorization before introducing controlled articles into a Security Area;
- Cooperate with Protective Force personnel during badge checks;
- Cooperate with Protective Force personnel during searches of vehicles, persons, and/or hand-carried items being brought into or out of a Security Area;
- Not remove or destroy any door cores or badge readers, unless the SOW in this Subcontract specifically indicates to do so;
- Not duplicate any keys issued;
- Store and protect all keys issued;
- Do not loan an assigned key to another worker without written authorization from the LANL Key Custodian;
- Return all issued keys to the responsible organization Key Custodian when no longer required and inform the RLM and STR/AdSTR of the same;
- *Immediately* report lost or stolen keys in person to the Key Custodian who issued the keys and inform the RLM and STR/AdSTR of the same;
- Adhere to all requirements for escorting individuals who are not authorized to be in a Security Area unescorted. (See Escorting, Section 4.2);
- Do not tailgate, piggyback, or vouch, nor allow another person to do so.

4.4 Acknowledgement / Control of Vehicles On-Site

- If requested, SUBCONTRACTOR shall submit to the STR/AdSTR or RLM the make, year and license number of all vehicles that will be used on site.
- Vehicles driven by unbadged drivers delivering construction materials or other supplies will be permitted to enter unsecured areas only if they are under escort by authorized DOE or LANL badged personnel.
- All non-government owned commercial vehicles and heavy duty vehicles (the equivalent of a Ford F350 or larger) will be screened by the Protective Force at the truck inspection station near the intersection of East Jemez Road and NM 4. If the search does not disclose anything of concern, the driver will receive an appropriate pass that will allow entry into their LANL destination.

4.5 Enhanced Security Areas

Subcontract Workers authorized to enter a Sensitive Compartmented Information Facility (SCIF), a Special Access Program Facility (SAPF), a certified Vault or Vault Type Room (VTR), a Material Access Area (MAA), a Protected Area (PA), or Limited Area (LA) with Special Administrative Access Controls shall comply with all training and other security requirements as directed by the LANL host organization and identified in the training matrix. These areas have rigid physical security standards and robust access controls that shall be adhered to.

4.6 Security Fences and Barriers

4.6.1 SUBCONTRACTOR shall make arrangements through the RLM or STR/AdSTR to ensure that adequate access control is maintained at any temporary openings or penetrations of Security Area boundaries. Such work shall be arranged through the RLM or STR/AdSTR and inspected/approved by the Physical Security Team or Deployed Security Officer to ensure there are adequate access controls in place during the temporary opening and that at the end of the work day the temporary openings are repaired / replaced. The RLM or STR/AdSTR shall provide the CA appropriate documentation related to SUBCONTRACTOR compliance with this requirement.

4.6.2 At the end of each work day or sooner if required, SUBCONTRACTOR shall repair, replace or provide adequate barriers to preclude unauthorized entry into any Security Area through temporary openings, penetrations, holes dug or cuts in security fences, or through modified gates or other alterations of security perimeters. The repairs shall be inspected / approved by the Physical Security Team or Deployed Security Officer at the end of the work day to ensure the temporary openings are repaired / replaced properly.

4.6.3 SUBCONTRACTOR shall make arrangements through the RLM or STR/AdSTR to ensure that any planned placement and proximity of equipment and vehicles to security fences and security boundaries does not create an unintended bridge to a Security Area.

G5.0 Personnel Security (May 2014)

5.1 Substance Abuse

The unauthorized use of alcohol and/or illegal drugs or being under the influence of alcohol and/or illegal drugs is prohibited on the LANL site. LANL's substance abuse policy applies to all who perform work at or for Los Alamos National Laboratory as a subcontract worker, guest scientist, visitor, student or other type of worker as it relates to ensuring a work environment that is free from unauthorized or illegal use, possession or distribution of alcohol or controlled substances.

Drugs currently used in CONTRACTOR'S pre-badging and random testing panel include marijuana, cocaine, opiates, heroine, phencyclidine and amphetamines. A detailed drug testing panel including cutoff concentrations can be found at http://www.lanl.gov/resources/_assets/docs/Exhibit-G/drug-testing-panel-2010.pdf

The use of medical marijuana is illegal under federal law and therefore is prohibited in accordance with these substance abuse requirements.

SUBCONTRACTOR shall ensure that Subcontract workers comply with all requirements of LANL's Substance Abuse Policy (SAP) which may be accessed electronically at http://www.lanl.gov/resources/exhibit-g.php.

For the purposes of this Exhibit, the term manager as used in the SAP means any or all of the following: STR/AdSTR, LANL manager or staff with oversight of this Subcontract, or on-site Subcontract personnel. Subcontractor workers found to be in violation of LANL's SAP may be restricted from working at the Laboratory.

SUBCONTRACTOR shall ensure that all lower-tier subcontractors meet the requirements of this section. Failure at any tier, of a SUBCONTRACTOR to comply with the requirements of this section, shall be grounds for the CONTRACTOR to bar the worker of a SUBCONTRACTOR at any tier from work on DOE/LANL property or on the subcontract.

5.1.1 Subcontract Workers shall:

- Be fit for duty and avoid behavior that compromises the health or safety of others or the security of the Lab;
- Notify Personnel Security, the RLM, STR/AdSTR and CA/PS immediately if cited, arrested or convicted of any drug or alcohol statute violation;
- Notify Personnel Security, the RLM, STR/AdSTR and CA/PS immediately if they are cited, arrested or convicted of any alcohol-related incident such as (e.g.) DUI, DWI, public intoxication, open container, minor in possession;
- Notify Personnel Security, the RLM, STR/AdSTR, and CA/PS immediately after any initiation of treatment for any drug or alcohol-related disorder (only required of workers with security clearances);
- Meet with Personnel Security or Occupational Medicine promptly when asked to perform a drug and/or alcohol test and fully cooperate with their instructions;

- Provide true and accurate records relating to their use of drugs and alcohol;
- Immediately report accidental ingestion of illegal drugs to Personnel Security, the RLM, and STR/AdSTR so the appropriate action can be taken.

5.1.2 Pre-badging Drug Testing

Subcontract workers who will obtain a standard (non-Visitor) badge such as a DOE Q, L, Un-cleared; Un-cleared Site-specific LANL; or Cleared/Un-cleared Foreign National badge, shall successfully pass a drug test no more than 60 days before obtaining a standard (non-Visitor) badge.

Subcontract workers who currently hold a standard badge but have not completed a pre-badge drug test, are required to complete the pre-badge drug test prior to working on a LANS subcontract for the first time.

Subcontract workers who currently hold a standard badge and transfer from one LANS subcontract to another without a break in service between subcontracts, are not required to complete a second pre-badge drug test.

Subcontract workers who hold a standard badge and experience a break in service for five (5) or more business days between LANS subcontracts are required to successfully pass a drug test no more than 60 days before re-obtaining a standard badge.

Subcontract workers shall not begin work on this subcontract until a pre-badging drug test is completed and passed, if applicable. The testing will be coordinated and paid for by SUBCONTRACTOR.

A drug testing laboratory used for any LANS required drug test shall be certified by the Department of Health and Human Services under the National Laboratory Certification Program. A current list of approved drug testing laboratories is published in the Federal Register which can be found at:
http://www.workplace.samhsa.gov/DrugTesting/Level_1_Pages/CertifiedLabs.html

SUBCONTRACTOR shall provide records of pre-badging drug screening to CONTRACTOR upon request.

5.1.3 Random Drug Testing

All Subcontract workers who are issued standard non-Visitor badges from the LANL Badge Office, which include Q, L or Un-cleared badges, are subject to random drug testing while on the LANL site.

Subcontract workers who are subject to random drug testing under another government testing program will not be included in LANL's random testing pool.

5.1.4 Reasonable Suspicion Drug and/or Alcohol Testing

5.1.4.1 When conducting reasonable suspicion testing, CONTRACTOR may test for any drug.

5.1.4.2 Drug and/or Alcohol testing will be required if:

- A Subcontract worker is reasonably suspected of being impaired by either drugs or alcohol.
- LANL Personnel Security, Occupational Medicine or LANL manager or supervisor determines that there is reasonable suspicion that the subcontract worker may have violated this procedure.
- The subcontract worker is the subject of a drug-detection dog alert and/or possesses property that has caused a drug-detection dog alert.
- A LANL manager or supervisor observes worker behavior commonly associated with alcohol or substance abuse such as unexplained chronic tiredness, tardiness, absence patterns, odor of alcohol, slurred speech, unsteady gait, etc. The manager or supervisor shall discuss the observed behavior with the worker as appropriate and make a referral to LANL Occupational Medicine for an evaluation of the worker.

5.1.4.3 Drug and/or alcohol testing may be required if:

- An incident or accident results in a serious injury or had the potential for serious injury occurs at work.
- LANL Occupational Medicine determines that unannounced, periodic testing is medically appropriate as indicated within the context of *Fitness for Duty* or *Human Reliability Program* monitoring.
- It is related to security clearances or applications for security clearances.
- When conducting occurrence testing, CONTRACTOR may test for any drug.

5.1.5 Other Testing

Drug and/or alcohol testing shall be required if:

- A non-vehicular incident or accident occurs at work that results in a serious injury or had the potential for serious injury.
- A vehicle accident that results in or had the potential for injury while driving any government-owned vehicle (including motorized equipment) on or off Laboratory property; or while driving any private vehicle (including rental vehicles) within the boundaries of a Laboratory Technical Area (other than downtown Los Alamos). [Note: Personnel Security will determine whether to require testing under these circumstances]
- It is necessary when related to security clearances or applications for security clearances.

5.1.6 Testing Conduct

CONTRACTOR'S Personnel Security organization has oversight of all drug and alcohol testing on-site at LANL for random, reasonable suspicion and other testing. All drug collections and alcohol testing are conducted in accordance with 49 CFR Part 40 and 10 CFR Part 707. All testing (except pre-badging drug testing) will be conducted and paid for by the CONTRACTOR.

5.1.7 Confirmed Positive Drug and/or Alcohol Test

The Requester or STR/AdSTR and LANL manager shall take the following actions if a Subcontract worker has a confirmed positive drug test:

- Immediately stop the worker from performing any additional work on site;
- Immediately notify Subcontract worker's management that the worker's badge is being pulled;
- Ask the worker to report back to his/her employer because his/her assignment is being terminated when a drug test is confirmed positive;
- Ask the worker to call a relative or friend to take him/her home when an alcohol test is confirmed positive;
- Confiscate the worker's badge and return it to Personnel Security;
- Consult with OM-MS to determine whether the worker should have a medical evaluation prior to driving;
- If alcohol related, instruct worker to report to OM-MS the next work day, prior to performing any work duties, for a Fitness for Duty evaluation unless the assignment is terminated.
- Coordinate with the CA/PS to ensure proper notifications are made regarding test results and any changes to the subcontract worker's assignment.

5.1.8 Failure to Show or Refusal of Drug and/or Alcohol Test

- If a worker fails to show up for a test after being contacted, such failure shall be treated in the same manner as a confirmed positive.
- If the worker refuses to be tested, such refusal shall be reported and treated as a confirmed positive.
- Failure to cooperate and submit to a drug/alcohol test shall be grounds for the CONTRACTOR to bar the worker from the LANL site and work on the subcontract.

5.1.9 Drug Detection Dogs may be used:

- On all Laboratory property (DOE-owned, leased or rented property for LANL) including, but not limited to parking lots.
- In and around worker's privately-owned vehicles parked on Laboratory property.
- In and around work areas.
- In and around desks, lockers and other containers assigned to workers.

5.1.9.1 If illegal drugs are found on a subcontract worker's person by using drug-detection dogs, the Requester or STR/AdSTR and LANL manager shall take action as outlined in Subsection 5.1.6.

5.1.9.2 If illegal drugs are not found, but the drug-detection dogs alert to the scent of illegal drugs in private property owned by a worker or in a work area, desk, locker or other container assigned to a certain employee and no illegal drugs are actually found, the LANL Physical Security Team shall notify the subcontract worker's LANL manager of a drug-detection dog alert. Additional action may be taken if behavior is observed by the LANL manager that may pose an immediate threat to the health and safety of the worker or others or a potential threat to security.

5.1.10 Off-site Behavior

The unlawful manufacture, distribution, dispensing, possession, use, transfer or sale of controlled substances is prohibited regardless of whether this occurs at the workplace, on Laboratory business, or on an individual's private time or property. These and other violations of this substance abuse policy are considered connected to work with or at LANL and may result in the termination of a Subcontractor worker's permission to work on DOE / LANL property or on the subcontract, regardless of whether or not the misconduct occurs during work hours or on Laboratory premises.

5.2 Badges

SUBCONTRACTOR shall ensure compliance with the badge requirements outlined in the following subsections. Any individual performing work under this subcontract shall obtain a DOE or LANL badge. (Subcontract workers, Guests and Affiliates)

All badges issued by the LANL Badge Office are accountable. Therefore, SUBCONTRACTOR shall ensure that every badge issued under this subcontract is returned to the LANL Badge Office. SUBCONTRACTOR shall also timely report any lost or stolen badges to the LANL Badge Office. Failure to return DOE security and site-specific (LANL) badges will result in denial of future badging services to the badge holder.

5.2.1 General Badging Requirements

5.2.1.1 A Subcontract Worker who is submitted for a standard DOE-Cleared or Uncleared badge or a LANL-Only Site-specific badge shall provide proof of U.S. citizenship to the LANL Badge Office at the time of badging. The foregoing applies regardless of the length of time that a Subcontract Worker will be on site.

5.2.1.2 Proof of citizenship includes an original photo identification card, such as a current and valid state driver's license and an original of one of the following five documents:

- For a worker born in the U.S., a birth certificate filed for record shortly after birth and certified with the registrar's signature is required. A delayed birth certificate (one created when a record was filed more than one year after the date of birth) is acceptable if it shows that the report of birth was supported by acceptable secondary evidence of birth. All documents submitted as evidence shall be original or certified.
- For a worker claiming citizenship by naturalization, a certificate of naturalization showing the individual's name is required.
- For a worker claiming citizenship acquired by birth abroad to a US citizen, one of the following (showing the worker's name) is required: Certificate of Citizenship issued by the Immigration and Naturalization Service; Consular Report of Birth Abroad of a Citizen of the United States of America (Form FS240); or Certificate of Birth (Form FS 545 or DS 1350).

- A US passport, current or expired; an expired passport is an acceptable proof of citizenship for badging purposes only.
- A record of Military Processing-Armed Forces of the US (DD Form 1966) provided it reflects that the worker is a US citizen.

5.2.1.3 A Subcontract Worker who is a US citizen, does not currently hold a DOE badge and meets applicable requirements, shall be issued a DOE Uncleared badge or LANL-Only Site-specific badge.

5.2.1.4 A Subcontract Worker who is either a Cleared or an Uncleared foreign national shall be badged in accordance with current DOE and LANL policies. The worker shall wear a photo badge whenever on DOE property (i.e. LANL) or LANL-leased premises.

5.2.1.5 Individuals who falsely certify their citizenship will be removed from the Laboratory and will be denied future access to LANL. This will be reported to the appropriate LANL organizations for investigation and other external organizations as necessary.

5.2.2 Obtaining a Badge

5.2.2.1 Worker (US Citizen) Requirements

- A worker shall obtain either a DOE or a LANL badge before performing any work at LANL.
- A worker shall present identification as required by the Badge Office before being issued a badge.

5.2.2.2 Official Visitor (US Citizen) Requirements

- An Official Visitor shall obtain a badge in accordance with this document;
- An Official Visitor shall wear a badge issued by the LANL Badge Office whenever on Laboratory Property;
- Uncleared Official Visitors will be required to sign a "*Statement of U.S. Citizenship*" form at the LANL Badge Office affirming their U.S. citizenship;
- Uncleared Official Visitors shall receive a briefing that covers safety and security requirements relevant to the work they will be performing;
- Uncleared Official Visitors who falsely certify their citizenship will be removed from the Laboratory and will be denied future access to LANL. This breach will also be reported to the appropriate LANL organizations.

5.2.2.3 Cleared Foreign National (Worker or Official Visitor) Requirements

A cleared foreign national, in conjunction with his or her Laboratory Host, shall contact the LANL Personnel Security Office to receive a cleared foreign national badge.

5.2.2.4 Uncleared Foreign National (Worker or Official Visitor) Requirements

An Uncleared foreign national, in conjunction with his or her Laboratory Host, shall contact the Foreign Visits & Assignment Team before performing work or other activities at LANL; and contact the LANL Personnel Security Office to receive an Uncleared foreign national badge.

5.2.3 Subcontract Workers shall:

- Complete training required by Personnel Security before receiving a badge (see Section 3.4.2 for training details);
- Wear the badge, photo-side out, above the waist, on the front side of the body, at all times while on DOE-owned property (i.e., LANL) or on CONTRACTOR leased or rented premises;
- Remove the badge and protect it from public view when leaving DOE-owned property or CONTRACTOR leased or rented premises;
- Present the badge whenever requested by Protective Force personnel, LANL host, or the Personnel Security Group;

- Not allow other individuals to use their badge under any circumstances;
- Minimize the number of instances of temporary badge issuance and replacement of lost badges;
- Ensure the badge is never photocopied;
- Return an issued badge to the Badge Office (via the RLM or STR/AdSTR as appropriate) following termination of employment, badge expiration, end of assignment, or completion of a visit. Subcontract Workers are not permitted to retain badges for any reason.
- Failure to return DOE security and LANL site-specific badges will result in denial of future badging services to the badge holder.

5.2.4 Badge Expiration Dates

5.2.4.1 Badges may be issued for the term of the subcontract. However, a SUBCONTRACTOR shall only request a badge for the period of time in which a Subcontract Worker will be utilized on this subcontract.

5.2.4.2 SUBCONTRACTOR shall abide by the following end date requirements:

- When a Subcontract Worker is working multiple subcontracts all outside of Security Areas, the earliest end date among the subcontracts will be the badge end date.
- When a Subcontract Worker holds a clearance (i.e., access authorization) under multiple subcontracts, the badge end date is based on the subcontract that is designated as the "primary" subcontract.
- When a Subcontract Worker holding a clearance (i.e., access authorization) is performing work under multiple subcontracts held by a Subcontractor that has received a favorable FOCI determination, the earliest end-date among those subcontracts is used. A new badge will need to be requested if there is any work to be performed that extends beyond the earliest end-date within a Security Area.

5.2.4.3 If a subcontract is going to be extended, SUBCONTRACTOR shall renew a Subcontract Worker's badge within 30 days prior to its expiration.

5.2.5 Lost or Stolen Badge(s)

5.2.5.1 Lost or stolen badges shall be reported to the Badge Office within 24 hours or the next business day after discovery of the loss, whichever is soonest. The RLM or STR/AdSTR shall also be notified. The individual badge holder shall go to the LANL Badge Office and complete a written affidavit (Form 1672) *Notification of Permanent Inactivation of Badge* in order to obtain a replacement badge.

5.2.5.2 In addition to 5.2.5.1, if a badge is stolen, the individual badge holder shall report the theft to the Security Incident Team (SIT) and inform the STR/AdSTR or CA/PS by the next business day of discovery of the loss.

5.3 Clearances (i.e., access authorizations)

SUBCONTRACTOR shall follow all clearance requirements outlined below and shall not permit any individual to have access to classified information; except when access to classified information is determined by proper clearance and the need-to-know.

The requirements for securing eligible personnel and proper personnel security clearances (i.e., access authorizations) for work within "L" and "Q" clearance areas and for complying with other security regulations and procedures shall not be considered cause for an extension of time for performance of the subcontract work or for extra payments under the subcontract. However, the cost of processing DOE "Q" or "L" access authorizations will be borne by the Government.

5.3.1 Requesting an Initial Clearance

SUBCONTRACTOR shall ensure that Subcontract Workers:

- Provide information required to request a clearance, including, but not limited to, proof of citizenship, Personal Identification Verification (PIV) documents, fingerprints, residence, work, education, military history, and personal references, as well as

specific information regarding any legal, financial, mental health or loyalty issues;

- Have had a complete a background investigation and testing for illegal drugs;
- Verify the Subcontract Worker's record is active in the system, correct and complete through the RLM or STR/AdSTR, including employer and subcontract number and that the worker is working on a FOCI approved contract;
- Complete a *Clearance Request/Recertification/Suitability Form* (DOE F 472.1C) signed by a LANL RLM.
- Complete an online (e-QIP) *Questionnaire for National Security Positions QNSP* (SF 86) and attendant clearance documents when requested by the Personnel Security Office.
- Meet with Clearance Processing Security Specialist and/or provide written responses to additional requests for information from Clearance Processing.

5.3.2 Clearance Processing Critical Reporting Elements

SUBCONTRACTOR shall ensure that subcontract workers holding a cleared DOE-standard badge, report any of the following events to Clearance Processing, the RLM and STR/AdSTR within **one (1)** working day of the occurrence unless otherwise stated:

- All arrests, criminal charges (including charges that are dismissed) or detentions by Federal, state, or other law enforcement authorities for violations of the law (other than traffic violations for which only a fine of $300 or less was imposed), within or outside of the US, unless the traffic violations were drug or alcohol related;
- Personal or business-related filing for bankruptcy;
- Garnishment of wages;
- Legal action effected for name change;
- Change in citizenship;
- Employment by, representation of, or other business-related association with a foreign or foreign-owned interest or foreign national;
- Any hospitalization for mental illness; treatment of drug abuse; or treatment for alcohol abuse;
- Approach or contact by any individual seeking unauthorized access to classified information or matter or SNM. If such an approach or contact is made while on foreign travel, workers should notify a Department of State official at the local US Embassy or Consulate;
- Termination of employment - also notify the RLM and STR/AdSTR;
- Change in duties resulting in a clearance no longer being required;
- Leave of absence or extended leave not requiring access to classified information or matter, or SNM for 90 consecutive working days;
- Leave for foreign travel, employment, assignment, education, or residence for more than three months, not involving official US Government business even if employment continues with the subcontractor.

5.3.3 Security Termination Requirements for Departing Subcontract Workers

Cleared Subcontract workers who are terminating work under a LANS Subcontract at the Laboratory for any reason shall meet all the federal and local requirements for departing workers.

Subcontract workers shall complete all clearance-related departure requirements. Some termination procedures are mandated by federal law. Failing to comply with the requirements can hinder or prevent a worker's future efforts to obtain a security clearance or badging services at LANL. Failure of a Cleared worker to follow proper termination procedures is also reported to NNSA/DOE by LANL Personnel Security.

Clearance-related requirements for departing Subcontract workers include the following:

- **Termination Briefing** - the Subcontract worker shall attend a termination briefing conducted by LANL Personnel Security or SUBCONTRACTOR management; and

submit a completed *LANS LLC Safeguards and Security Clearance Termination Briefing Form* to Personnel Security.

- **Security Termination Statement** - the Subcontract worker shall sign and submit a *Security Termination Statement* DOE Form 5631.29 to LANL Personnel Security.
- **Surrender DOE Access Credentials** - the Subcontract Worker shall surrender his or her security badge to the LANL Badge Office, while coordinating with the RLM and STR/AdSTR.

For each event listed below, the required action shall be carried out within **two (2**) **working days** of the Event described in the first column of the table.

Event	Do Termination Briefing & Form, and Submit DOE Form 5631.29	Return These Badges
Subcontract Worker's employment terminated	Individual Subcontract Worker	Subcontract Worker's badge, whether Cleared or Uncleared, including expired
Subcontract Worker transferred from subcontract	Individual Subcontract Worker	Subcontract Worker's badge, whether Cleared or Uncleared, including expired
Clearance no longer required	All Subcontract Workers	All Cleared "L" or "Q" badges, including expired
Subcontractor's FOCI approval withdrawn or terminated	All Subcontract Workers	All Cleared "L" or "Q" badges, including expired
Subcontract completed or terminated	All Subcontract Workers	All badges, whether Cleared or Uncleared, including expired

- SUBCONTRACTOR shall ensure that any Subcontract Worker who holds a clearance and is no longer working on this subcontract, follows the security clearance termination process outlined above.
- SUBCONTRACTOR shall notify Personnel Security, the RLM, STR/AdSTR and CA/PS of any Event that changes the status of a worker's need for a badge.

5.3.4 Clearance Renewals or Reinvestigations

SUBCONTRACTOR shall ensure that a Subcontract Worker whose clearance is being renewed or reinvestigated:

- Completes the reinvestigation e-QIP package every 5 years for Q clearance holders or every 10 years for L clearance holders.
- Completes the LANL Annual Security Refresher Training before the effective date of the training expiring and access is therefore denied.

5.4 Foreign Ownership, Control or Influence (FOCI)

FOCI determinations are required for a SUBCONTRACTOR, its owners, and lower-tier subcontractors, if a subcontract requires Q or L-cleared access authorizations. Before a Subcontract Worker may be Q or L-cleared, his/her company shall undergo a FOCI certification. A separate FOCI determination is required for a prime subcontractor and any lower-tier subcontractor.

SUBCONTRACTOR'S Key Management Personnel shall have an active clearance or a clearance request in process before a favorable FOCI determination can be returned. As a part of the FOCI determination process, SUBCONTRACTOR'S Facility Security Officer (FSO) and any additional workers with security responsibilities shall complete the self-study course indicated under Section 3.4.2.

SUBCONTRACTOR shall submit their FOCI packages / information online at this website: https://foci.anl.gov/. A favorable FOCI determination shall be rendered prior to LANL granting a facility clearance requiring access authorizations. Questions related to FOCI should be addressed through the RLM or STR/AdSTR to the Personnel Security POC.

5.4.1 SUBCONTRACTOR shall ensure that the following notifications are immediately provided to the Personnel Security POC and the RLM or STR/AdSTR.

- Written notification of a change in the extent and nature of FOCI that affects the information in the FOCI determination;
- Immediately provide written notification and supporting documentation relevant to changes that would affect the information in a subcontractor's or any tier parents' most recent DOE FOCI submission(s).

5.4.2 SUBCONTRACTOR shall complete and submit a new FOCI package at least every five years or at the request of CONTRACTOR, to the Personnel Security POC.

5.4.3 SUBCONTRACTOR shall certify annually to the Personnel Security POC and inform the RLM or STR/AdSTR and the CA/PS that:

- No significant changes have occurred in the extent and nature of FOCI that would affect the answers to the questions provided in it's FOCI representations;
- No changes have occurred in the organization's ownership;
- No changes have occurred in the organization's officers, directors, and executive personnel.

5.4.4 CONTRACTOR may terminate this subcontract for default if SUBCONTRACTOR either fails to meet obligations imposed by this section, or creates a FOCI situation in order to avoid performance or a termination for default. CONTRACTOR may terminate this subcontract for convenience if SUBCONTRACTOR becomes subject to FOCI and for reasons other than avoidance of performance of the subcontract, cannot, or chooses not to avoid or mitigate the FOCI problem.

5.5 Human Reliability Program

SUBCONTRACTOR shall comply with all requirements of the Human Reliability Program (HRP) if they have workers who take part in the program.

5.5.1 SUBCONTRACTOR shall ensure that Subcontract Workers who are HRP certified shall:

- Hold a DOE security clearance;
- Submit to testing for illegal drugs;
- Submit to testing for alcohol abuse;
- Submit to random polygraph examinations;
- Complete medical and psychological evaluations which require a polygraph examination;
- Complete Part 2 of the QNSP annually;
- Complete initial and annual HRP training (see Section 3.4.2 for details)

5.5.2 SUBCONTRACTOR shall ensure that Subcontract Workers shall be enrolled in HRP if their work responsibilities involve:

- Access to Category I SNM or transportation or protection of Category I quantities of SNM;
- Nuclear explosive duties or responsibility for working with, protecting, or transporting nuclear explosives, nuclear devices or selected components;
- Access to information concerning vulnerabilities in protective systems when transporting nuclear explosives, nuclear devices, selected components or Category I quantities of SNM; or
- The potential to significantly impact national security or cause unacceptable damage to national security.

5.5.3 Removal from HRP

5.5.3.1 A RLM who has a reasonable belief that an HRP-certified Subcontract Worker is not reliable, based on either a safety or security concern, shall immediately remove the Subcontract Worker from HRP duties pending a formal determination of the individual's reliability.

5.5.3.2 Subcontract Workers may be placed on a temporary removal for a safety or security concern by a supervisor / manager, LANL oversight manager or the HRP management official.

A safety concern means any condition, practice, or violation that causes a substantial probability of physical harm, property loss, and/or environmental impact.

A security concern means the presence of information regarding an individual applying for or holding an HRP position that may be considered derogatory. Such information may include, but is not limited to:

- Observable phenomena, such as direct observation of the use or possession of illegal drugs or alcohol;
- The physical symptoms of being under the influence of drugs or alcohol;
- A pattern of abnormal conduct or erratic behavior;
- Information provided by a reliable and credible source that is independently corroborated; or
- Detection of alcohol odor on the breath.

5.5.3.3 An HRP-certified individual who is removed completely or placed on temporary removal is prohibited from entering any Material Access Areas and shall immediately stop performing HRP duties.

5.6 Foreign Visits and Assignments

5.6.1 On-Site work

All foreign national Subcontract workers are required to have approval to work on-site from the LANL Foreign Visits and Assignments office PRIOR to their arrival at the Laboratory. Foreign national Subcontract workers shall be issued a security badge before performing work at LANL. They will be required to present a valid passport and visa documentation before a badge will be fabricated and issued. The individual who is hosting a foreign national on-site shall be a CONTRACTOR employee and a US citizen.

5.6.2 Off-site work

Approval for a foreign national to work off-site on a LANL project is not required if the following conditions are met: 1) all work is conducted entirely off-site and 2) the research results from this Subcontract are open, non-sensitive and will be published in open literature intended for public release. If either of the above criteria is not met, approval for a foreign national to work on a LANL project off-site must be obtained prior to commencing work on this Subcontract as outlined in Section 5.6.1.

G6.0 Information Security (May 2014)

Subcontract workers shall not disclose LANL data collected, created, processed, transmitted, stored or disseminated by SUBCONTRACTOR in performance of this subcontract, unless each case of such disclosure is specifically approved by the LANL Data Owner and the CA/PS.

Subcontract workers shall ensure LANL data utilized in the performance of this subcontract is not used for any other purpose that has not been specifically approved by the LANL Data Owner.

6.1 Official Use Only (OUO) and LANS Proprietary (LPI) Information

OUO and LPI information is unclassified with the potential to damage government, commercial or private interests if disseminated to persons who do not have a need-to-know the information.

Personal Identifiable Information (PII) is a type of OUO. PII is any information collected or maintained by DOE or CONTRACTOR about an individual, including but not limited to education, medical history, financial transactions and employment history; and information that can be used to distinguish an individual's identity.

SUBCONTRACTOR shall protect OUO and LPI information from unauthorized dissemination (e.g. to persons who do not require the information to perform work under this subcontract) and shall follow all requirements for OUO and LPI documents specified below.

6.1.1 Access

No security clearance is required for access to OUO or LPI.

If OUO information is Export Control Information (ECI) access is restricted to US persons, defined as citizens and Lawful Permanent Residents. Access to ECI (including parts,

tools, material and equipment fabricated from ECI specifications and drawings) by non-Permanent Resident Alien foreign nationals is prohibited.

If OUO information is Applied Technology (AT) it is subject to access restrictions established by the DOE Program Office. The associated LANL program manager can determine access authorizations for Laboratory workers.

6.1.2 Storing

OUO and LPI information shall be stored in a locked room or locked receptacle (e.g. desk, file cabinet, safe). OUO information stored on a computer shall meet all LANL password, authentication, encryption, or file access control requirements.

6.1.3 Reproduction

All copies of LANL OUO and LPI (including 3-D print prototypes) must be protected, accessed, stored, marked, transmitted and destroyed in the same manner as the originals.

6.1.4 Transmitting

E-mail messages that contain OUO or LPI information should indicate OUO or LPI in the first line, before the body of the text. OUO or LPI disseminated over networks outside of LANL should be encrypted with NIST-validated encryption software (e.g., Entrust®).

PII information that is disseminated over networks outside of LANL shall be encrypted with NIST-validated encryption software

In the case of hard copies being sent outside of LANL OUO or LPI shall be placed in a sealed, opaque envelope marked with the recipient's name, a return address and the words "To Be Opened by Addressee Only". For interoffice mail within LANL, OUO or LPI shall be placed in a sealed, opaque envelope with the recipient's address and the words "To be Opened by Addressee Only" on the front of the envelope.

6.1.5 Destroying

Users are not required to destroy electronic media that contains OUO or LPI. However, disks should be overwritten using approved software before they are thrown away. Hard copy OUO or LPI documentation shall be destroyed by using an approved shredder (strips no more than ¼ inch wide).

6.1.6 Export Controlled Information Restrictions

The work to be performed under this subcontract includes LANL technical data; the export of which is restricted by the Arms Export Control Act (22 U.S.C. §2751, et seq.), the Atomic Energy Act of 1954, as amended (42 U.S.C. §2011) or the Export Administration Act of 1979, as amended (50 U.S.C. §2401, et seq.). Violations of these laws may result in severe administrative, civil, or criminal penalties. Further dissemination must be pre-approved by Los Alamos National Laboratory.

6.2 Unclassified Controlled Nuclear Information (UCNI)

UCNI is certain unclassified but sensitive government information whereby unauthorized dissemination is prohibited. UCNI is intended to be viewed only by those individuals with a need-to-know. SUBCONTRACTOR shall protect such information from unauthorized dissemination and shall follow all requirements for UCNI documents specified below.

6.2.1 Access

No security clearance is required for access to UCNI; however, access is permitted only to those authorized for routine or special access and those who have a need-to-know. UCNI stored on a computer shall be restricted (passwords, authentication, file access control encryption and offline storage) to only those who have a need-to-know.

6.2.2 Storing

When using UCNI, physical control shall be maintained over the material to prevent unauthorized access to the information. When not in use, UCNI matter shall be stored in a locked room or receptacle (e.g. desk, file cabinet, bookcase or safe). The locked receptacle shall have controls that limit access to only approved workers. UCNI stored on a computer shall meet all LANL password, authentication, encryption or file access control

requirements.

6.2.3 Transmitting

Ensure that UCNI is marked correctly prior to transmitting it over any media. Only a qualified Reviewing Official can identify and mark UCNI. Contact the Classification Group through the RLM or STR/AdSTR for assistance.

When transmitting over telecommunication circuits (including telephone, fax, radio, e-mail or Internet) encryption algorithms that comply with all applicable Federal laws, regulations, and standards for the protection of UCNI shall be used.

Transmission over open phone lines is prohibited. A Secure Terminal Equipment (STE) line is required. All cellular devices, including LANL-issued smart phones such as Blackberries must be turned off completely when in proximity to UCNI discussions.

UCNI documents shall be transmitted using a fax machine that employs encryption. When transmitted via fax or e-mail outside LANL, UCNI shall be encrypted with NIST-validated encryption software. E-mails with UCNI attachments are considered transmittal documents and shall be marked and encrypted as such.

If mailing outside of LANL, an opaque envelope shall be used and the outer packaging shall not indicate that the content within is UCNI. For interoffice mail, an interoffice envelope shall be used and mailed through standard interoffice mail, but do not indicate that the content is UCNI. When using e-mail, UCNI shall be encrypted with NIST-validated encryption software such as Entrust®.

6.2.4 Destroying

Users are not required to destroy electronic media that contain UCNI. Disks should be overwritten using approved software before they are discarded. Hard copy UCNI documents are to be destroyed by shredding in an approved shredder (cross-cut particles no larger than ¼ inch wide and 2 inches long). SUBCONTRACTOR shall coordinate with the Classified Matter Protection and Control Team through the RLM or STR/AdSTR to properly destroy UCNI information.

6.2.5 Noncompliance Consequences

SUBCONTRACTOR'S failure to comply with the requirements pertaining to UCNI may result in the imposition of a civil and/or criminal penalty for each violation.

6.3 Classified Matter and Material

Disclosure of any classified information relating to the work or services hereunder to any person not entitled to receive it, or failure to safeguard any classified information, may subject the SUBCONTRACTOR, its agents, employees or lower-tier subcontractors to criminal liability under the laws of the United States (i.e., Atomic Energy Act of 1954, as amended, 42 U.S.C 2001 et seq.; 18 U.SC. 793 and 794; and Executive Order 12958).

6.3.1 General Responsibilities

6.3.1.1 SUBCONTRACTOR shall ensure compliance with all requirements for accessing, storing, generating, marking, reproducing, receiving, transmitting, and accounting for classified matter documents and materials.

6.3.1.2 SUBCONTRACTOR shall employ need-to-know controls, safeguard all classified information and protect against sabotage, espionage, loss or theft of the classified documents and material in SUBCONTRACTOR'S possession in connection with the performance of work under this subcontract.

6.3.1.3 Except as otherwise expressly provided in this subcontract, SUBCONTRACTOR shall, upon completion or termination of this subcontract, transmit to CONTRACTOR all classified matter in the possession of all Subcontract Workers.

6.3.2 Classified Matter Responsibilities

Subcontract Workers shall:

- Complete required CMPC training, before receiving access to classified matter;

- Protect classified matter from unauthorized physical, visual or aural access;
- Ensure classified matter in use shall be constantly attended by, or under the control of, a person possessing the proper access authorization and need-to-know.
- Conduct classified discussions and classified work only in Security Areas;
- Conduct classified discussions or classified work that involves Top Secret (TS) information only in a Security Area specifically approved for TS;
- Discuss, release, or transmit Classified Matter only to those individuals possessing the required clearance and need-to-know;
- Ensure that Classified Matter is attended or stored in an approved security container;
- Ensure when classified information is discussed, ensure that the classification level and category and any applicable caveats are stated before the discussion begins.
- Immediately report any issues concerning missing classified matter, emergency situations, controlling or transmitting classified matter to the SIT, DSO or SPL and LANL RLM.

6.3.3 Determining Need-to-Know

Any Subcontract Worker who has been granted access to classified matter shall determine another worker's clearance and need-to-know before granting access to that matter. Need-to-know shall be established by:

- determining what matter will be accessed; and
- determining whether the recipient requires access to this matter to perform his / her official duties through current relationships, tasks, duties and assignments or confirmation by a LANL RLM.

6.3.4 Clearance requirements for access to classified matter:

Category & Level of Classified Matter	Q Cleared	L Cleared
Confidential National Security Information	Permitted	Permitted
Confidential Formerly Restricted Data	Permitted	Permitted
Confidential Restricted Data	Permitted	Permitted
Secret National Security Information	Permitted	Permitted
Secret Formerly Restricted Data	Permitted	Permitted
Secret Restricted Data	Permitted	Excluded
Top Secret National Security Information	Permitted	Excluded
Top Secret Formerly Restricted Data	Permitted	Excluded
Top Secret Restricted Data	Permitted	Excluded
Sigmas 14 & 15 granted by UCSC or alternate		

6.3.5 Training Requirements for Classified Matter Users

All Subcontract Workers who access, generate, handle, store or process classified matter shall take the following training: (See Section 3.4.2 for details)

Course Title	Frequency
Classified Matter Protection	Once
CMPC User Refresher Training	24 months

Specific training is required for any Subcontract worker who will be working with Sigma 14, 15 or 20 classified matter. These workers shall take the following training as it applies to their job duties within the scope of work: (See Section 3.4.2 for details)

Course Title	Frequency
Sigma 14 Awareness	12 months
Sigma 15 Awareness	12 months
Sigma 20 Awareness	12 months

6.3.6 Marking Classified Matter

Properly marking classified matter is complicated and situation specific. If a Subcontract Worker is going to be working with classified documents, the RLM or STR/AdSTR shall arrange for the Subcontract Worker to take the appropriate training in this area.

6.3.7 Storing Classified Matter

When storing Classified Matter, Subcontract Workers shall:

- Store classified matter that is not in use in an approved security container.
- Return all classified matter to the LANL RLM or other authorized personnel if a Subcontract Worker will be on leave for more than 90 days, no longer needs to use the classified matter, or terminates employment.
- Protect Classified Matter that is pending Derivative Classifier review at the highest potential or possible classification level and category.
- Ensure combinations on containers on LANL property are changed as required.
- Secure security containers before leaving such containers unattended.
- Perform end-of-day checks to ensure proper storage of Classified Matter.

6.3.8 Requirements for Storage of Classified Matter

6.3.8.1 Secret and Confidential matter shall be stored in: a locked GSA-approved safe within a Security Area; or in a certified Vault or Vault Type Room within a Security Area.

6.3.8.2 Top Secret (TS) matter shall be stored in: a locked GSA-approved safe in a Security Area with supplemental controls approved by the Physical Security Team; or in a certified Vault or Vault Type Room approved for TS by the Physical Security Team.

6.3.9 Receiving or Transmitting Classified Matter

6.3.9.1 Classified mail shall be delivered to a primary or alternate CMC at the designated classified mail stop with the inner envelope unopened. All incoming classified mail shall be examined for evidence of tampering, incorrect addressing, improper marking, improper transmission and incorrect packaging.

6.3.9.2 Prior to sending classified matter, Subcontract workers shall verify the intended recipient's clearance or access authorization, any required program or special access approvals, need-to-know for the matter being transmitted, and approved classified mail address. Workers shall ensure the classified matter is marked in accordance with LANL procedures (CMPC Handbook).

6.3.10 Destroying Classified Matter

6.3.10.1 Subcontract Workers shall destroy unneeded (e.g. multiple copies) or obsolete classified matter and classified was as soon as practical. Classified matter covered by any current moratoriums or court orders shall not be destroyed. Record copies of documents, whether electronic or paper-based shall only be destroyed in accordance with established Laboratory records retention requirements and procedures.

6.3.10.2 Classified matter shall be destroyed using only approved destruction equipment located within a Limited Area or higher. Classified matter shall be destroyed beyond recognition to prevent reconstruction. Acceptable methods for destroying classified matter include shredding, pulping, melting, mutilation, chemical decomposition, or pulverizing.

G7.0 Cyber Information Security (Feb 2014)

These requirements apply to any information system or network that SUBCONTRACTOR may use to collect, create, process, transmit, store or disseminate information for CONTRACTOR. Unless specifically waived, CONTRACTOR retains ownership of the data that SUBCONTRACTOR may utilize in performance of this subcontract. Regardless of the performer of the work, SUBCONTRACTOR shall ensure compliance with the provisions of this section.

7.1 Cyber Information Security Training

7.1.1 On-site for more than 10 days per year

A Subcontract worker who will be on-site more than 10 days per year and will have access to a LANL computer, network or system shall complete the Initial Computer Security Briefing as soon as access is granted to LANL information system resources. All Subcontract workers who are on-site more than 10 days shall also complete Annual Security Refresher training. New users may have access to training systems in the Badge Office in the Otowi Building or at the White Rock Training Center.

All Subcontract workers required to take the Initial Information Security Briefing will also be required to complete the Annual Information Security Refresher each year.

All other required Cyber Information Security training identified in the table below shall be completed prior to computer access and prior to performing the assigned function that the training prepares the Subcontract Worker to perform. See Section 3.4.2 for additional details.

Course Name	Frequency	All Computer Users	Classified Computer Users	Training Type
General Employee Training (GET)	One time	X	X	Live
Initial Information Security Briefing	One time	X	X	Web
Annual Information Security Refresher	12 months	X	X	Web
Classified Computer Security Briefing	One time		X	Web

7.1.2 On-site for less than 11 days per year

A Subcontract worker who will be on-site for 10 days or less per year and will have access to a LANL computer, network or system may participate in live training with the appropriate OCSR, ISSO or other Cyber Information Security specialist based upon the requirements of the statement of work. If a subcontract worker requires access to LANL's Yellow Network during the performance of this subcontract, a Cyber Information Security specialist may accompany and oversee the worker.

7.2 CONTRACTOR Responsibilities

7.2.1 Informing the LANL Data Owner

The LANL Data Owner(s) will inform the SUBCONTRACTOR of the sensitivity and classification of data that may be utilized in performance of this subcontract. See Section 6.0 requirements.

7.2.2 Specifying Protection Requirements

The LANL Cyber Information Security Office will specify information protection requirements appropriate to the sensitivity/classification of all data SUBCONTRACTOR may utilize in performance of this subcontract.

7.3 General Subcontract Worker Responsibilities

7.3.1 Data Sensitivity Determination

Subcontract workers shall ensure that the LANL Data Owner has specified the data sensitivity and/or classification of all data that will be collected, created, processed, transmitted, stored or disseminated by SUBCONTRACTOR. SUBCONTRACTOR shall ensure its workers are knowledgeable of the data classification associated with this subcontract. See Section 6.0 requirements.

7.3.2 Approvals

Subcontract workers shall obtain specific approval from the LANL Cyber Security Office prior to connecting any equipment owned or acquired by SUBCONTRACTOR to any LANL network, with the coordination of the STR/Ad/STR.

7.3.3 Accountability

Subcontract workers shall be accountable for their actions on an information system.

7.3.4 Acknowledge Responsibilities

Subcontract workers shall acknowledge their responsibilities for protecting information systems and electronic information and for complying with any system-specific rules of use. Acknowledgement will be captured during the Initial Information Security Briefing.

7.3.5 Ensure Control of Media

Subcontract workers shall ensure that system media and system output are properly classified, marked, controlled and stored.

7.3.6 Follow the Rules and Regulations

Subcontract workers shall follow rules and regulations governing the secure operation and authorized use of information systems (CONTRACTOR, SUBCONTRACTOR and sub-tier).

7.3.7 Periodic Assessments

Subcontract workers shall submit at the discretion of the LANL Cyber Security Office to a periodic assessment to be performed by the LANL Data Owner as to the effectiveness of the information protection mechanisms identified that are implemented by SUBCONTRACTOR.

7.3.8 Non-Disclosure

Subcontract workers shall not disclose LANL data collected, created, processed, transmitted, stored, or disseminated by SUBCONTRACTOR in performance of this subcontract, unless each case of such disclosure is specifically approved by the LANL Data Owner and the CA/PS.

7.3.9 Media Control and Destruction

7.3.9.1 Subcontract workers shall contact the LANL OCSR or ISSO and STR/AdSTR when information storage media (such as hard drives, removable storage media or non-volatile memory devices) is no longer needed or required for this subcontract.

- The decision whether to clear, sanitize and destroy the unclassified storage media shall be made by the LANL OCSR or ISSO;
- Coordinate with the LANL OCSR or ISSO for the destruction of non-classified CDs, DVDs, or flash drives etc., and the handling, marking and destruction of classified CDs, DVDs or flash drives etc.;
- All classified media shall be brought into accountability and destroyed.

7.3.9.2 Subcontract workers shall ensure LANL data utilized in the performance of this subcontract is not used for any other purpose that has not been specifically approved by the LANL Data Owner, including testing of new systems or applications or demonstrations of software or systems for the purpose of marketing the SUBCONTRACTOR'S skills or services to customers other than LANL.

7.3.10 Non-Government Owned Classified Systems

Subcontract workers shall ensure any subcontractor activity that involves processing LANL classified information using a non-government owned information system be documented and approved by the LANL Cyber Security Office before access is granted.

7.4 Reporting Requirements

SUBCONTRACTOR shall report when the following conditions arise:

7.4.1 System is no Longer Required

Immediately inform the ISSO or OCSR and STR/AdSTR when access to a particular information system is no longer required (i.e., completion of the subcontract, transfer from the subcontract, or removal from the Subcontract).

7.4.2 Security Incidents

Report all potential information security incidents to the Security Incident Team at 505-665-3505. Reports of potential Information security incidents (Cyber Information Security related) after business hours and on weekends shall be made in accordance with Section 3.6.2. Use caution when reporting an incident involving classified information or classified systems through insecure means. Never report over the phone or through e-mail.

7.5 On-site System and Data Access Requirements As a minimum, SUBCONTRACTOR shall comply with the following requirements regarding all levels of LANL data (classified and unclassified) and PII:

7.5.1 System Certification for Mandatory Protected Information

If SUBCONTRACTOR will be processing LANL mandatory protected information (PII, UCI, UCNI, and other sensitive unclassified data) on SUBCONTRACTOR'S systems, certification of the SUBCONTRACTOR'S system(s) by Cyber Information Security (through a Memorandum of Agreement or Subcontractor Security Plan) is required.

7.5.2 Non-Disclosure Agreement

If SUBCONTRACTOR will have access to LANL sensitive unclassified and/or classified information and data, SUBCONTRACTOR will be required to sign a *Non-Disclosure Agreement*, before access to data or information is provided by the LANL Cyber Information Security Office.

7.5.3 Access Control Protections

Ensure that authentication mechanisms, including passwords, issued for the control of their access to information on information systems are not shared, are protected at the same level of protection applied to the information to which they permit access, and that any compromise or suspected compromise of an authenticator is reported to the appropriate ISSO or OCSR and STR/AdSTR.

7.5.4 Visual Protections

Protect terminals from unauthorized access as described in the appropriate Cyber Information *System Security Plan*.

7.5.5 Authentication Requirements

Utilize robust, preferably two-factor authentication when granting users access to the data SUBCONTRACTOR may utilize in performance of this subcontract.

7.5.6 Data Encryption

Utilize encryption, when specified by the LANL Cyber Information Security Office, performed by a product listed in the NIST FIPS 140-2 validated products list (http://csrc.nist.gov/cryptval/).

7.5.7 Use of Least Privilege Principle

Grant user access to LANL data using the least privilege principle; which ensures that Subcontract Workers are granted only the access privileges absolutely necessary to accomplish the work specified by this subcontract.

7.5.8 Access to Classified Information

Ensure access to classified information is granted only to persons with the appropriate access authorization (clearance) and need-to-know in the performance of their duties under this subcontract.

7.5.9 Access to Unclassified Information

Ensure access to unclassified information is granted only to persons who have a need-to-know for the information in the performance of their duties under this subcontract;

7.6 Off-site Access to LANL Systems

7.6.1 Generally, only LANL and U.S. government owned information systems may process government sensitive information - e.g. LANL information. In rare instances, approval can be granted for non-government owned systems to process and store LANL mandatory protected information.

7.6.2 Non-government collaborators or other entities that own intellectual property, used or developed in joint work with LANL, do not need permission to store that data on non-government owned devices.

7.6.3 Remote users who do not process mandatory protected information may access LANL systems by fulfilling the following requirements.

7.6.3.1 Access to LANL systems from Off-site

To obtain access to LANL systems from off-site, SUBCONTRACTOR shall:

- Be approved to receive a CRYPTOCARD [Foreign Nationals must have approval from LANL Foreign Visits & Assignments before requesting a CRYPTOCARD – See G5.6.1];
- Shall apply for off-site access (*Off-Site User Responsibility Form 2146)*;
- Obtain approval from the LANL RLM with CSSM concurrence.

7.6.3.2 Remote Users

SUBCONTRACT workers shall ensure the following operational controls are implemented:

- Authenticate with single-use passcodes; with a one-time use password list or a CRYPTOCARD generated passcode;
- Close the browser before leaving the remote system;
- Ensure files from off-site systems have been examined for malicious content (e.g. anti-virus or anti-spyware) before introduction to a LANL information system;
- Ensure virus definition file on off-site computer is the most recent version;
- Ensure any sensitive information that was transmitted to the remote system is protected;
- Classified information shall not be processed during remote access sessions and is prohibited on any computer that is not approved for classified processing.

7.6.4 Violating remote access requirements outlined above may result in the loss of access to on-site, as well as off-site computing. Other actions may be taken up to and including removal of the Subcontract work from this subcontract.

7.7 Off-site Storage of LANL Sensitive Data on Subcontractor's Systems

7.7.1 Approval Requirements

SUBCONTRACTOR shall have approval from the LANL Cyber Information Security when storing and processing LANL sensitive and mandatory protected information on SUBCONTRACTOR'S systems.

7.7.2 Certification of Protection Measures

LANL Cyber Information Security will confirm that the system's protection measures have been correctly implemented in accordance with LANL's information security planning process.

7.8 Cloud Computing Services SUBCONTRACTOR shall comply with cloud computing services requirements outlined in the following subsections for the use of cloud services. A cloud service denotes any connection that involves delivering host services over the Internet.

7.8.1 Qualification and Validation

SUBCONTRACTORS shall comply with the following regulations and requirements:

- National Institute of Science Technology (NIST 800-53) found at http://csrc.nist.gov/publications/PubsSPs.html or equivalent approved by the CSSM
- Federal Information Processing Standard (FIPS) Publication 199 found at http://csrc.nist.gov/publications/PubsFIPS.html
- A Cloud Computing Security Plan may be required prior to services beginning f

Compliance with these requirements shall be verified by LANL Cyber Information Security prior to SUBCONTRACTOR submitting a formal response to a Request for Proposal.

SUBCONTRACTOR shall complete a Cloud Service Security Requirement Questionnaire as part of the review and approval process which can be found at http://www.lanl.gov/resources/_assets/docs/Exhibit-G/cloud-services-security-requirements-questionnaire-rev2.pdf
Only those subcontractors who meet the minimum qualifications shall be authorized to provide service.

7.8.2 Certification and Accreditation

SUBCONTRACTOR shall develop, with the assistance of the LANL Information Cyber Security Office, the following plans prior to the use of a cloud service. These plans must be approved by LANL Cyber Information Security before an Approval to Operate notice is issued.

If SUBCONTRACTOR is already federally authorized or industry tested and authorized, additional certification or accreditation is not required. Supporting documentation will still be required.

- Configuration Management Plan
- Contingency Plan
- System Security Plan or equivalent
- Privacy Impact Assessment (if LANL PII is going to be stored)

SUBCONTRACTOR shall provide results of bi-annual and annual security control test results to the LANL Information Cyber Security Office. A list of the control tests required can be found at http://www.lanl.gov/resources/_assets/docs/Exhibit-G/nist-800-53.pdf.

7.9 Classified Scanning

SUBCONTRACTOR shall comply with enhanced security requirements for document scanning activities to prevent compromising classified information. Scanners include secure copiers connected to secure networks, secure copiers connected to secure desktop systems, secure scanners connected to automated information systems, and secure multi-function scanners.

7.9.1 System Accreditation

All classified equipment shall be accredited before processing classified information. The LANL Cyber Security Office shall approve the use of all non-government owned equipment prior to processing classified information.

7.9.2 Operator Training

Secure scanner operators shall complete training in Classified Matter Protection and Control and Classified Cyber Information Security including:

- Annual Security Refresher Briefing
- Classified Matter Protection
- Computer Security Annual Refresher
- Classified Computer Security Briefing
- Sigma 15 training, if applicable
- Reading Section 3.4 “Reproducing Classified Matter” and Attachment A “Rules of Use and Operating Instructions” in the Classified Matter Protection and Control Handbook, P204-2.

7.10 Consequences of Noncompliance

Failure of SUBCONTRACTOR to comply with the requirements of Section G7.0 may result in the imposition of a criminal and/or civil penalty. Activities on LANL systems are monitored and recorded and subject to audit. Use of LANL systems and data is expressed consent to such monitoring and recording. Any unauthorized access or use of LANL systems and data is prohibited and could subject the SUBCONTRACTOR to criminal and civil penalties.

G8.0 Controlled Articles / Wireless Technology (Feb 2014)

LANL’s level of control on wireless computing devices and on other controlled articles depends on the type of device, who owns it (Government or non-Government), where it will be located and how it will be used.

8.1 Controlled Articles

Controlled Articles are stand-alone devices that can store, read, write, record or transmit data. Certain controlled articles can read and/or write nonvolatile information and plug into a computer. They are not stand-alone devices like other types of controlled articles.

Controlled articles are not permitted in Security Areas without prior authorization. SUBCONTRACTOR shall ensure that controlled articles are not brought into a Security Area without prior written approval from the Cyber Information Security Office with concurrence by the RLM or STR/AdSTR. Additional LANL site-specific requirements may exist and shall be followed as appropriate.

Controlled articles include:

- Cell phones, smart phones, cordless phones, Blackberry devices, two-way pagers, two-way radios;
- Recording equipment (audio, video, optical, or data);
- Copiers or scanners with hard drives;
- Radio frequency (RF) transmitting equipment (including ankle monitoring devices), Infrared (IR) or other wireless transmission capabilities;
- Electronic equipment with a data exchange port capable of being connected to automatic information system equipment;
- Portable computers, including but not limited to: laptops, tablet computers, personal digital assistant (PDAs), palm-top computers, Blackberry devices, Notebooks, iPhones or iPads;
- Portable electronic reading, web-browsing and data collection devices with WiFi or USB connectivity, including but not limited to: Kindles, iPads, Nextbook Tablets, Nook eReaders, Sony Digital Readers or iPods;
- Any device with a capability to connect to computers or use wireless communications;
- Cameras - video, still, digital, film, tablet computers or in cell phones. If the use of cameras - either inside or outside of a Security Area is deemed mission essential - then use of cameras shall be authorized via coordination with the STR/AdSTR, the RLM and the Physical Security Team prior to the use of such cameras. *(Form 1897PA)* A Subcontract worker using a non-government owned camera on Laboratory property shall possess a valid DOE/LANL badge.
- CD / DVD write drives
- External hard drives
- Flash memory (i.e. PC cards, SD memory cards)
- USB memory devices (i.e. thumb drives, memory sticks, jump drives)

8.2 Approvals Required Before Commencement of Work

8.2.1 Prior to the introduction of any controlled articles into a Limited Area or connected to a LANL-owned system, approval shall be obtained from the Cyber Information Security Office. The RLM or STR/AdSTR shall also be informed.

8.2.2 Prior to any wireless operation on wireless projects (unclassified or classified) approval shall be obtained from LANL's Cyber Information Security Office. The RLM or STR/AdSTR shall also be informed. Violations of this requirement may constitute a security infraction, and may result in administrative actions up to and including exclusion of a Subcontract Worker from LANL and/or from working on this subcontract.

8.2.3 Subcontractors using wireless technology, including construction sites, need to obtain certification and approval from the Cyber Information Security Office prior to engaging wireless technology. A LANL "Wireless System Security Plan" may also be required.

8.3 Rules for Using Authorized Controlled Articles in Security Areas

Authorized controlled articles with audio recording or data transmitting capabilities in Security Areas shall be turned off (for UCNI), batteries removed (for classified) or placed in an approved Radio Frequency container whenever:

- A classified or UCNI discussion or phone call is taking place within audible range;
- Classified or UCNI computer processing is taking place in the immediate area of the device;
- Classified or UCNI faxing is taking place within the immediate area of the device; and
- Classified or UCNI copying is taking place on a digital copier in the immediate area of the device.

It is the responsibility of subcontract workers to be cognizant of classified or UCNI activities that may be occurring in adjacent work areas. Workers shall confirm that no classified or UCNI activities area taking place in the immediate vicinity prior to using the authorized controlled article.

8.4 Wireless Device Requirements

8.4.1 The use of devices with wireless connectivity such as computing, cellular and printing devices with “Bluetooth” technology, or wireless networking protocol is prohibited anywhere at LANL, including all LANL property and leased space except for certain defined areas. Wireless devices cannot be connected to LANL computing assets or networks. Such capabilities shall be disabled unless the activity has been approved by the LANL Cyber Information Security Office. It is the user’s responsibility to know what devices they possess, the capabilities of those devices and to ensure that wireless capabilities have been disabled.

8.4.2 The use of wireless networking, Bluetooth and cell phone technologies is allowed in public areas of the Bradbury Science Museum, the Otowi Cafeteria and public access areas outside buildings such as roadways, sidewalks and parking lots.

8.4.3 The use of wireless networking is not restricted in non-LANL occupied areas of LANL-leased properties such as Canyon Complex, White Rock Training Center, the Research Park and Central Park Square.

8.4.4 These wireless device requirements do not apply to the wireless computing capability used by Subcontractor delivery and shipping workers in the LANL receiving area outside of a building.

8.4.5 Active wireless devices that have prior approval to be in a PPA and/or Limited Area shall be labeled (company sticker, owner’s name) to identify Subcontractor ownership.

8.5 LANL and Government-owned Wireless Devices

8.5.1 Government-owned cell or satellite phones shall be disabled when inside a Limited Area or higher Security Areas.

8.5.2 All LANL and government-issued cellular devices including smart phones such as Blackberries shall be turned off completely when in proximity to UCNI activity. Batteries must be removed when in proximity to classified activity.

8.5.3 Only LANL-issued Blackberry devices, applications and accessories may be carried in Limited Areas. No Blackberry devices are allowed in Vault Type Rooms, SCIFs or SAPFs.

8.5.4 Government-owned computing controlled articles (e.g. laptops, palmtop computers and PDAs) shall follow access control requirements such as username and password.

8.5.5 Government-owned computing controlled articles shall use anti-virus software to detect malicious activity where the capability exists.

8.5.6 Government-owned unclassified controlled articles are not permitted to connect to any LANL computer or network or store LANL sensitive data without approval from LANL management. *(Form 1865)*

8.6 Non-government Owned Controlled Articles

8.6.1 Non-government owned controlled articles are prohibited in Limited Areas and higher security areas.

8.6.2 All non-government owned cellular devices including smart phones such as Blackberries shall be turned off completely when in proximity to UCNI activity. Batteries must be removed when in proximity to classified activity.

8.6.3 Non-government owned controlled articles may not be connected to any LANL-owned information system or network (classified or unclassified) without written approval and may not be used to store any sensitive or classified government information without written approval. *(Form 1897)*

8.6.4 Non-government owned controlled articles shall not store or process government controlled unclassified information; unless formal approval has been granted and full disc encryption is utilized.

8.6.5 When privately-owned vehicles are allowed to enter a Limited Area, controlled articles that are attached to the vehicle (i.e. built-in cell phones, On Star and CB radios) shall be turned off if capable and left in the vehicle. Additional restrictions may apply in some areas and Subcontract workers shall follow local controls.

8.7 Non-government Wireless Computing Devices

8.7.1 LANL management approval may be required before bringing a non-government computing device (e.g. laptop, Tablet computer, iPhones, iPad) to a Property Protection Area based on local security requirements. *(Form 1897)*

8.7.2 LANL Cyber Information Security Office approval is required if computing devices will be in a Security Area or connected to the LANL network. *(Form 1897)*

8.7.3 LANL management approval is required before connecting a non-government computing device to a LANL network. *(Form 1897)*

8.7.4 Non-government owned wireless computing devices shall be authorized prior to connecting to any LANL wireless computing resource.

8.8 Connecting to Presentation Systems and Using Equipment Remote Controls

8.8.1 Non-government owned controlled articles may be connected to stand-alone presentation equipment and stand-alone systems in PPAs provided:

8.8.1.1 The information system has virus detection software active, automatically scanning for malicious code and using the most current definition file and,

8.8.1.2 The information system shall not contain any sensitive information that the controlled article owner does not have authorization to access.

8.8.2 LANL prohibits Radio Frequency (RF) keyboards everywhere.

8.8.3 LANL allows RF and Infrared (IR) remote controls on unclassified presentation equipment (audio, video, etc.) in unclassified workspace without restrictions.

8.8.4 LANL does not allow RF and IR remote controls on classified computers.

8.8.5 IR and RF remote controls are permitted to control projectors.

G9.0 Contacts (May 2013)

Name	Telephone	Email
ADSS After-hours On-call Officer cell phone	505-699-4094	
ADSS After-hours On-call Duty Officer pager	505-949-0156	
Badge Office	505-667-6901	badge@lanl.gov
Chief Information Office (CIO)	505-606-2263	
Chief Information Office on-call pager	505-664-6282	
Classification Group	505-667-5011	
Classified Matter Protection & Control	505-665-1802	cmpc@lanl.gov
Clearance Processing	505-667-7253	clearance@lanl.gov
Counterintelligence Program	505-665-6090	
(Cyber) Information Security Help Desk	505-665-1795	cybersecurity@lanl.gov
Emergency Management & Response	505-667-6211	
Fire, Bomb Threat, etc.	911	
Foreign Ownership Control & Influence	505-665-1624	
Foreign Visits and Assignments	505-665-1572	
Fraud, Waste and Abuse	505-665-6159	
Immigration Services	505-667-8650	
Info Security Operations Center (iSOC) Coordinator Pager	505-949-4762	
Lock Shop	505-667-4911	
Material Control & Accountability Group	505-667-5886	
Network Operations Center (NOC)	505-667-7423	noc@lanl.gov
Operations Security Program Office (OPSEC)	505-665-4843 or 505-667-0002	
Personnel Security	505-665-6565	
Physical Security Team	505-667-2510	
Protective Force	505-667-4437	

Name	Telephone	Email
Protective Force After Hours Reporting (Central Alarm Station)	505-665-7708	
Protective Force After Hours Shift Commander	505-665-1279	
Safety Help Desk	505-665-7233	
Security Help Desk	505-665-2002	security@lanl.gov
Security Incident Team (SIT)	505-665-3505	
Wireless Point of Contact		wirelesssecurity@lanl.gov

G10.0 Required Notifications (Dec 2007)

SUBCONTRACTOR shall notify the Requester, STR/AdSTR and the Contract Administrator /Procurement Specialist immediately, whenever a change in the scope of the work to be performed has been identified or requested. The Requester or STR/AdSTR shall then notify the appropriate security expert so that any security modifications can be made to the approved Exhibit G in response to the change in the scope of work.

Attachment G1

EXHIBIT "G"
SECURITY REQUIREMENTS
Vendor Name (if Applicable): *
P.R. No. *
Ex. G dated: *

REQUIRED REVIEWS AND APPROVALS

Sections G1 - G6, G8 - G10 & Questionnaire (if applicable) Reviewed By:

Name of DSO or SPL	Signature	Date

Section G7 Reviewed and Approved By:

Name (Cyber) Information Security	Signature	Date